



K-Shield Jr.

NCS 기반 실무형 정보보호 기술인력 양성

K-Shield Jr. 정보보호 관리진단 과정 5기

[프로젝트 결과 발표]

모의해킹 2팀

OO 홈페이지(OO)

모의 해킹 진단결과

- 01. 취약점 진단
- 02. 시나리오 예상
- 03. 취약점 대처 방안
- 04. 우선순위

INTRODUCTION

정형수

팀장

1996.11.11

010-2626-7867

jhs1142002@gmail.c
om

김재원

팀원

1996.04.12

010-7131-1771

wjswls45645697@gmail.
com

김상훈

팀원

1997.01.12

010-5198-9792

t3rr3t@kakao.com

이호웅

팀원

1992.04.13

010-6231-9426

dlghdnd@gmail.com

취약점 진단

회원정보 유출 및 취약점

홈페이지 취약점



01 회원정보 유출 및 취약점

- 크로스 사이트 스크립팅(XSS)
- 불충분한 인증
- 불충분한 인가
- 데이터 평문 전송
- 세션 고정
- 프로세스 검증 누락
- 쿠키 변조



02 홈페이지 취약점

- 디렉터리 인덱싱
- 정보노출
- 자동화 공격
- 관리자 페이지 노출
- 불충분한 세션 만료
- 파일 업로드
- 파일 다운로드
- SQL 인젝션

×

회원정보 유출 및 취약점

01

크로스 사이트 스크립팅(XSS)

악의적인 사용자가 공격하려는 사이트에
스크립트를 실행시켜 사용자의 민감한 **정보 탈취**
가능하다.

발생 경로

OO

시나리오

해커가 의도한 악의적 스크립트가 삽입된 사이트 접속
을 유도하여 악성코드 감염을 시킬 수 있고 세션 값을
탈취하여 계정의 권한을 탈취할 수 있다.

공지사항

KISEC Album

F-NGS Lab

수강후기

공지사항

제목 > ' <script>alert();</script>' 검색

| 번호 | 제목 | 등록일 |
|----|------------------|----------------|
| 3 | test입니다 | 2020 . 10 . 27 |
| 2 | 테스트 파일입니다. | 2020 . 08 . 18 |
| 1 | KISEC 홈페이지 구성 완료 | 2020 . 08 . 18 |

확인

크로스 사이트 스크립팅(XSS)

악의적인 사용자가 공격하려는 사이트에
스크립트를 실행시켜 사용자의 민감한 **정보 탈취**
가능하다.

보호 대책

- 소스코드 수정(문자 필터링 또는 치환)

프로그래밍을 할 시 사용자가 문자열에 스크립
트를 삽입하여 실행하는 것을 막기 위해 사용자
가 입력한 문자열에서 < , > 를 필터링하여 치환
한다.

| From | To |
|------|------|
| < | < |
| > | > |



불충분한 인증

인증 절차가 불충분한 경우 발생하는 취약점으로 권한이 없는 사용자가 중요 정보 페이지에 접근하여 정보를 유출하거나 변조 가능하다.

발생 경로

OO

시나리오

중요 정보의 수정 및 탈퇴에 2차적인 인증이 없어 계정의 권한이 없는 공격자가 CSRF공격을 활용하여 특정 사용자의 정보를 수정하거나 회원 탈퇴 처리가 가능하다.

회원정보수정

나의 강의실

1:1문의

회원탈퇴

일반회원 정보수정

회원가입으로 다양한 교육 서비스를 제공 받으세요.
고객님께 해당되는 유형을 선택하세요

이름

aaaa

휴대폰

010

▼

1234

1234

회원정보수정

나의 강의실

1:1문의

나의 쿠폰함

회원탈퇴

회원탈퇴

사이트의 불편하신 사항이나 건의하고자 하는 사항 그리고 칭찬하고자하는 모든 상호아들을 이곳에 남겨주시면 빠른 시일 내에 답변드리겠습니다.

아이디

aaaa@kisec.com

패스워드

패스워드 확인

탈퇴내용

불충분한 인증

인증 절차가 불충분한 경우 발생하는 취약점으로 권한이 없는 사용자가 중요 정보 페이지에 접근하여 정보를 **유출하거나 변조** 가능하다.

보호 대책

[민감한 정보 접근 2차인증]
민감한 정보 수정이 이루어지는 페이지의 사용자 비밀번호 재확인과 같은 **2차적으로 인증 가능한 프로세스**를 추가한다.

[패스워드 규칙 서버측 확인]
클라이언트에서만 패스워드 규칙을 확인하는 것이 아니라 전송된 값을 **서버에서도 규칙 부합 여부**를 판단하는 프로세스를 추가한다.

| | | | | | | | | | | | | | |
|--------|--|---------|----------------|--|--|------|-----|---------|------|------|--|--|--|
| 회원정보수정 | <h3>일반회원 정보수정</h3> <p>회원가입으로 다양한 교육 서비스를 제공 받으세요. 고객님께 해당되는 유형을 선택하세요.</p> <table><tr><td>이름</td><td colspan="3">aaaa</td></tr><tr><td>휴대폰</td><td>010</td><td>1234</td><td>1234</td></tr></table> | 이름 | aaaa | | | 휴대폰 | 010 | 1234 | 1234 | | | | |
| 이름 | aaaa | | | | | | | | | | | | |
| 휴대폰 | 010 | 1234 | 1234 | | | | | | | | | | |
| 회원정보수정 | <h3>회원탈퇴</h3> <p>사이트의 불편하신 사항이나 건의하고자 하는 사항 그리고 칭찬하고자하는 모든 상호아들을 이곳에 남겨주시면 빠른 시일 내에 답변드리겠습니다.</p> <table><tr><td>아이디</td><td colspan="3">aaaa@kisec.com</td></tr><tr><td>패스워드</td><td></td><td>패스워드 확인</td><td></td></tr><tr><td>탈퇴내용</td><td colspan="3"></td></tr></table> | 아이디 | aaaa@kisec.com | | | 패스워드 | | 패스워드 확인 | | 탈퇴내용 | | | |
| 아이디 | aaaa@kisec.com | | | | | | | | | | | | |
| 패스워드 | | 패스워드 확인 | | | | | | | | | | | |
| 탈퇴내용 | | | | | | | | | | | | | |

불충분한 인가

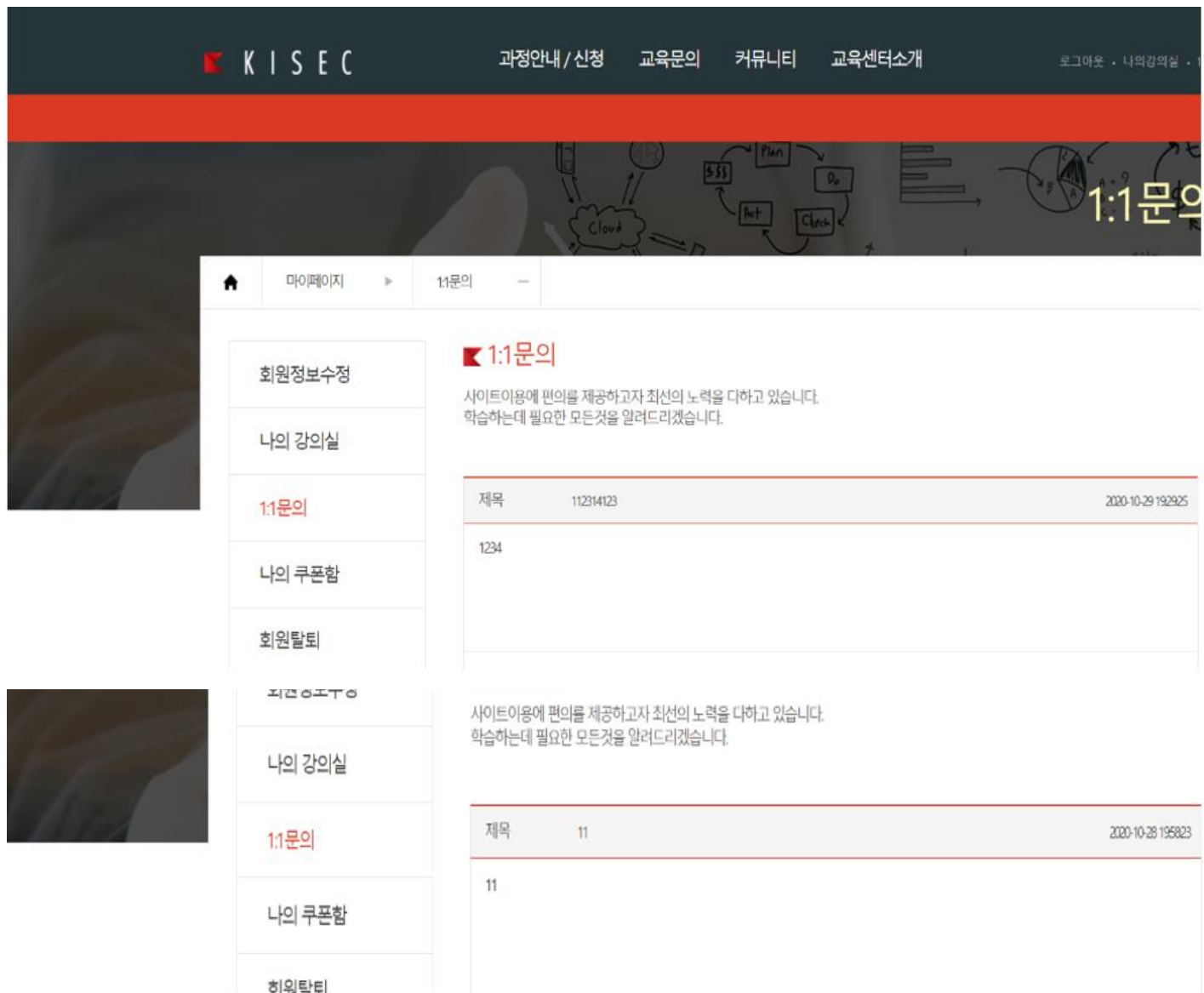
인증 로직이 구현되지 않을 경우, 비인가 사용자의 페이지에 접근 및 중요 정보의 **열람 및 변조**가 가능하다.

발생 경로

OO

시나리오

인가되지 않은 공격자가 권한이 없는 1대1문의 내용을 확인할 수 있고 수정할 수 있다. 그러한 내용을 확인하면서 개인 정보를 탈취당할 수 있고 그로인한 2차피해가 발생한다.

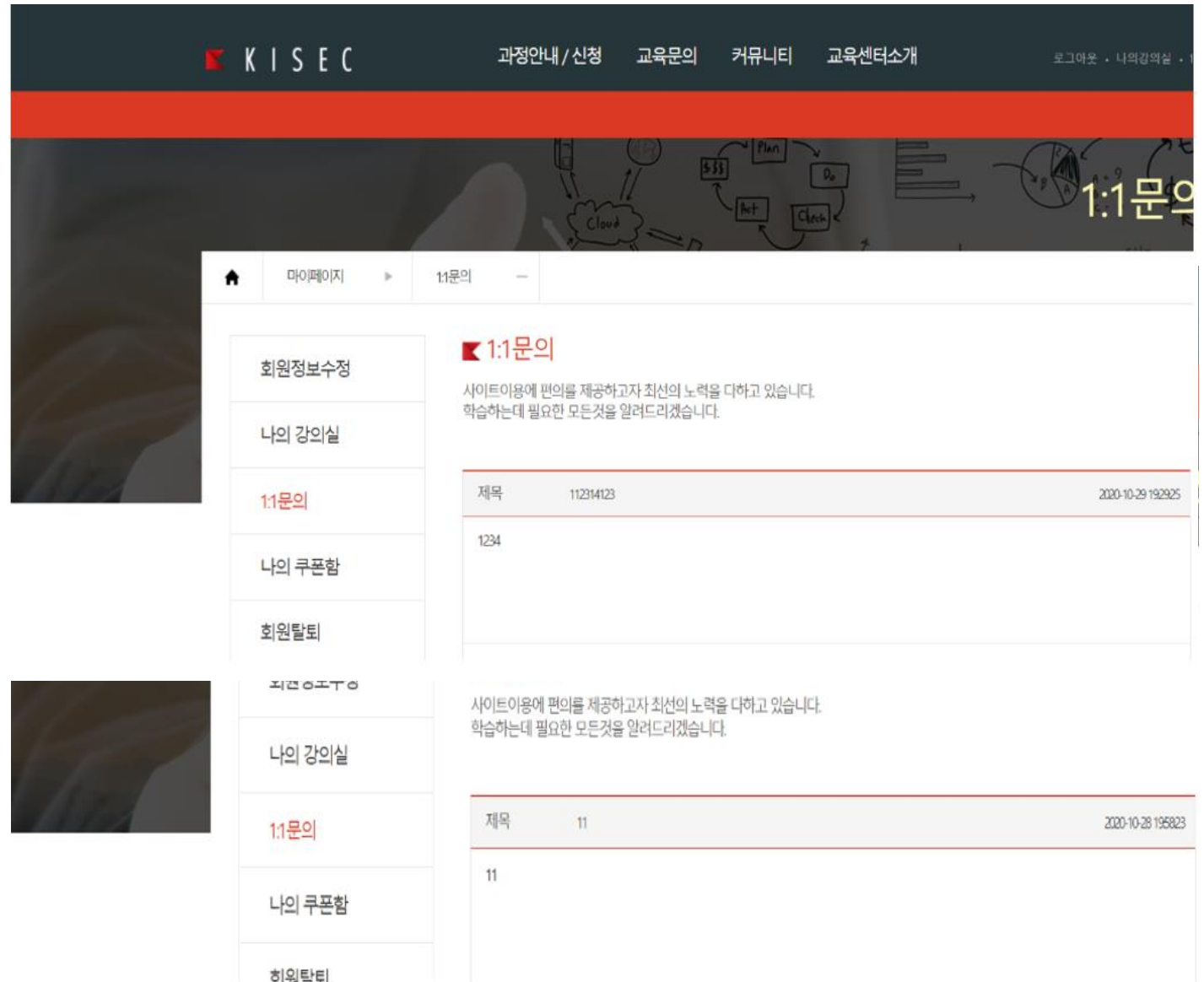


불충분한 인가 - 2

인증 로직이 구현되지 않을 경우, 비인가 사용자의 페이지에 접근 및 중요 정보의 열람 및 변조가 가능하다.

발생 경로

OO

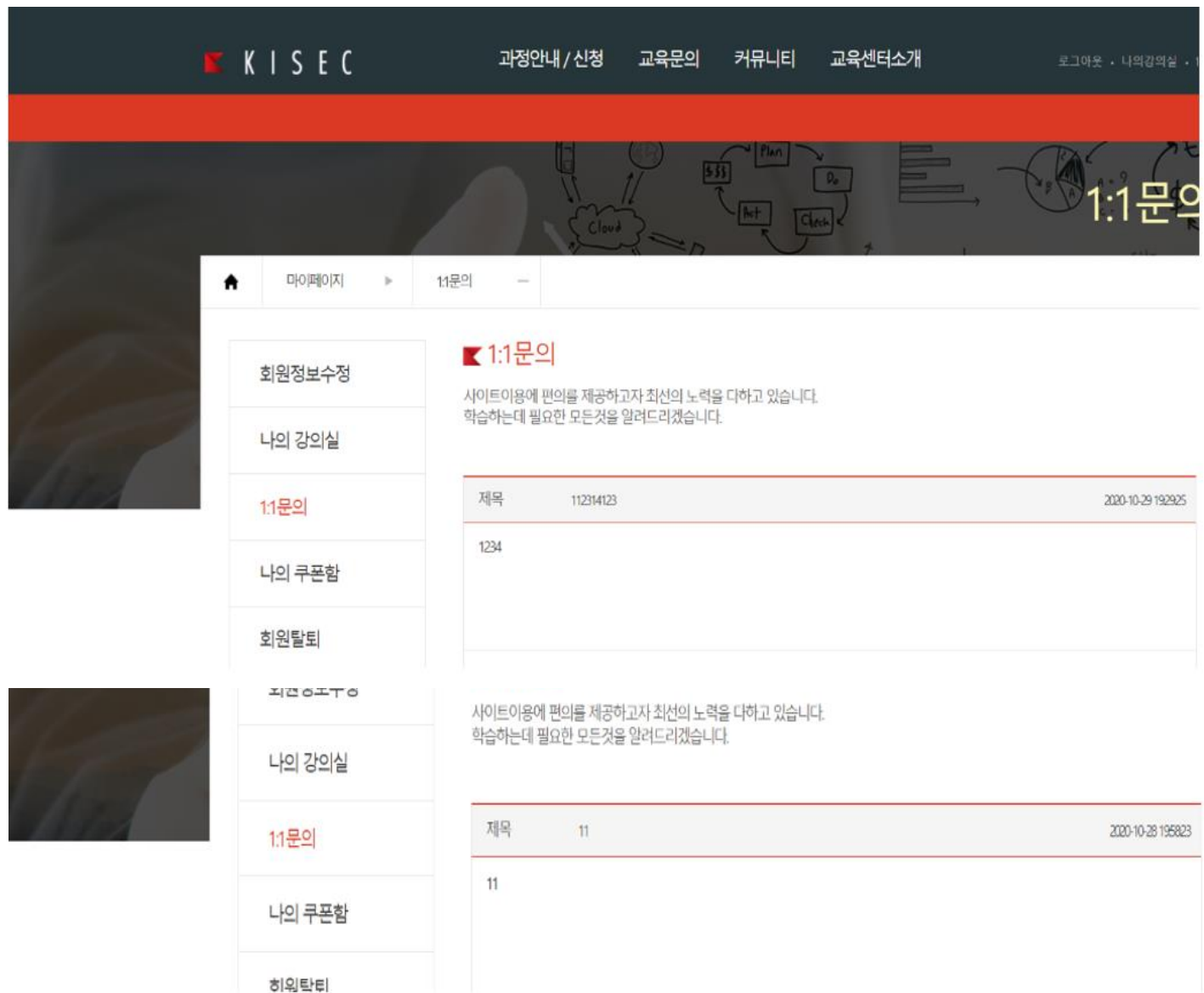


불충분한 인가

인증 로직이 구현되지 않을 경우, 비인가 사용자의 페이지에 접근 및 중요 정보의 **열람 및 변조**가 가능하다.

보호 대책

- 소스코드 수정(세션인증)
프로그래밍을 할 때 세션인증이 필요한 페이지에는 세션인증을 하는 코드를 삽입하고, **세션이 존재하지 않다면 접근이 불가능하게** 설정해야 한다.
- 프로그래밍 예시
인증 과정을 처리하는 부분에 Client Side Script(Javascript, VBScript 등)를 사용하면 사용자가 임의로 수정할 수 있으므로 Server Side Script(ASP, PHP, JSP)를 통하여 **인증 및 필터링 과정**이 수행되어야 한다. 불가피하게 사용 시 반드시 암호화하여 사용하고 **서버 측에서 무결성**을 검증해야 한다.



데이터 평문 전송

Mode=login&login_email=aaaa%40kisec.com&login_pw=test123!HTTP/1.1 200 OK

서버와 클라이언트간 통신 시 암호화하여 전송을 하지 않아 중요 정보 등이 **평문**으로 전송되는 취약점이다.

발생 경로

OO

시나리오

로그인시 아이디와 비밀번호를 전송하는데 암호화하여 전송을 하지 않아 공격자가 중간에 탈취하여 로그인을 할 수 있다.
그로 인해 회원정보가 유출되고 2차피해가 발생한다.

```
-----115620926220389056261172985294
Content-Disposition: form-data; name="mm_cell_1"

010
-----115620926220389056261172985294
Content-Disposition: form-data; name="mm_cell_2"

1234
-----115620926220389056261172985294
Content-Disposition: form-data; name="mm_cell_3"

1234
-----115620926220389056261172985294
Content-Disposition: form-data; name="emailID"

tess
-----115620926220389056261172985294
Content-Disposition: form-data; name="emailDomain"

kisec.com
-----115620926220389056261172985294
Content-Disposition: form-data; name="select"

kisec.com
-----115620926220389056261172985294
Content-Disposition: form-data; name="user_pass"

tess123!
-----115620926220389056261172985294
Content-Disposition: form-data; name="re_pass"

tess123!
-----115620926220389056261172985294
Content-Disposition: form-data; name="mm_company"

-----115620926220389056261172985294
Content-Disposition: form-data; name="mm_grade"
```


데이터 평문 전송 2

서버와 클라이언트간 통신 시 암호화하여 전송을 하지 않아 중요 정보 등이 **평문**으로 전송되는 취약점이다.

발생 경로

OO

```
user_id=bbbb%40kise.com&user_idx=1407&Mode=secede_member&user_pass=test123!&re_pass=test123!  
&withdrawal=%ED%83%88%ED%87%B4%ED%85%8C%EC%8A%A4%ED%8A%B8HTTP/1.1 200 OK
```

```
up_member  
-----267201677623251230708934036  
Content-Disposition: form-data; name="mm_email"
```

```
bbbb@kise.com  
-----267201677623251230708934036  
Content-Disposition: form-data; name="old_pass"
```

```
3b3e9bf9e01962fe4fb9ef658533392e  
-----267201677623251230708934036  
Content-Disposition: form-data; name="mm_name"
```

```
bbbb  
-----267201677623251230708934036  
Content-Disposition: form-data; name="mm_phone_1"
```

```
0  
-----267201677623251230708934036  
Content-Disposition: form-data; name="mm_cell_2"
```

```
1234  
-----267201677623251230708934036  
Content-Disposition: form-data; name="mm_cell_3"
```

```
1234  
-----267201677623251230708934036  
Content-Disposition: form-data; name="mm_company"
```

```
coupnag  
-----267201677623251230708934036  
Content-Disposition: form-data; name="mm_grade"
```

```
daeri  
-----267201677623251230708934036--
```

데이터 평문 전송

서버와 클라이언트간 통신 시 암호화하여 전송을 하지 않아 중요 정보 등이 **평문**으로 전송되는 취약점이다.

보호 대책

개인정보(아이디, 비밀번호, 주민등록 번호, 전화번호, 계좌번호, 계좌 비밀번호, 게시판 등에서 사용되는 성명, 이메일, 연락처 등)를 다루는 사이트는 SSL 인증서, 또는 암호화 응용프로그램을 설치하여 개인정보 **암호화 송·수신**을 해야 한다

```
user_id=bbbb%40kisec.com&user_idx=1407&Mode=secede_member&user_pass=test123!&re_pass=test123!&withdrawal=%ED%83%88%ED%87%B4%ED%85%8C%EC%8A%A4%ED%8A%B8HTTP/1.1 200 OK
```

```
-----115620926220389056261172985294
Content-Disposition: form-data; name="mm_cell_1"

010
-----115620926220389056261172985294
Content-Disposition: form-data; name="mm_cell_2"

1234
-----115620926220389056261172985294
Content-Disposition: form-data; name="mm_cell_3"

1234
-----115620926220389056261172985294
Content-Disposition: form-data; name="emailID"

tess
-----115620926220389056261172985294
Content-Disposition: form-data; name="emailDomain"

kisec.com
-----115620926220389056261172985294
Content-Disposition: form-data; name="select"

kisec.com
-----115620926220389056261172985294
Content-Disposition: form-data; name="user_pass"

tess123!
-----115620926220389056261172985294
Content-Disposition: form-data; name="re_pass"

tess123!
-----115620926220389056261172985294
Content-Disposition: form-data; name="mm_company"


-----115620926220389056261172985294
Content-Disposition: form-data; name="mm_grade"
```



세션 고정


세션값을 고정하여 세션 식별자(ID) 값으로 사용자가 로그인하여 정의된 세션 식별자(ID)가 사용 가능하게 되는 취약점이다.


발생 경로
OO


시나리오
세션값이 고정되어 있기 때문에 각 사용자별 세션ID를 탈취할 수 있으면 공격자가 접근 및 권한 우회가 가능하여 회원정보 유출이 발생한다.



값
kjt6cj47t46nbklbdch49ar4



도메인



도메인



값
1234124123123124124124


도메인


도메인


값
kjt6cj47t46nbklbdch49ar4


도메인

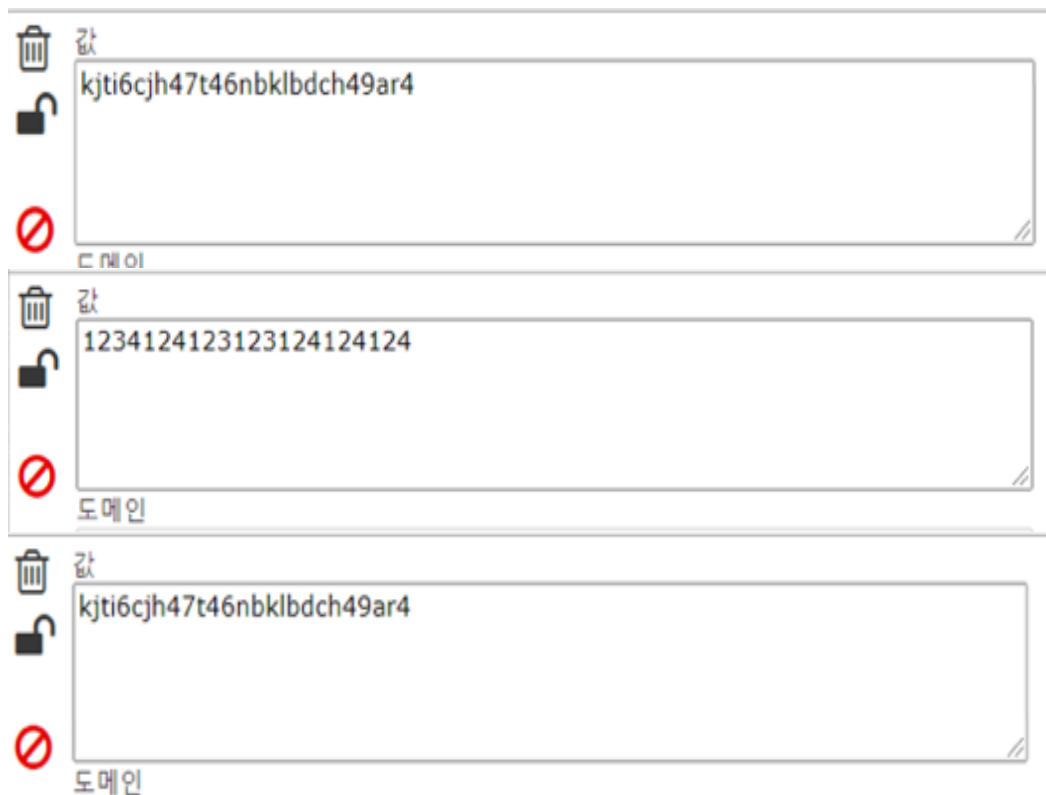

도메인

세션 고정

세션값을 고정하여 세션 식별자(ID) 값으로 사용자가 로그인하여 정의된 세션 식별자(ID)가 사용 가능하게 되는 취약점이다.

보호 대책

로그인과 같은 인증절차가 진행된 후 인증된 세션은 신규 세션 발행을 하여 탈취된 세션이 주입하여도 **우회 할 수 없도록 조치**하여야 한다. 만약 신규 세션을 발행할 수 없는 경우에는 인가시점에 쿠키상에 별도의 **토큰**을 발행하여 매 요청별로 세션영역에 보관된 토큰과 매칭을 시키는 방법 또한 하나의 방법이다.



프로세스 검증 누락

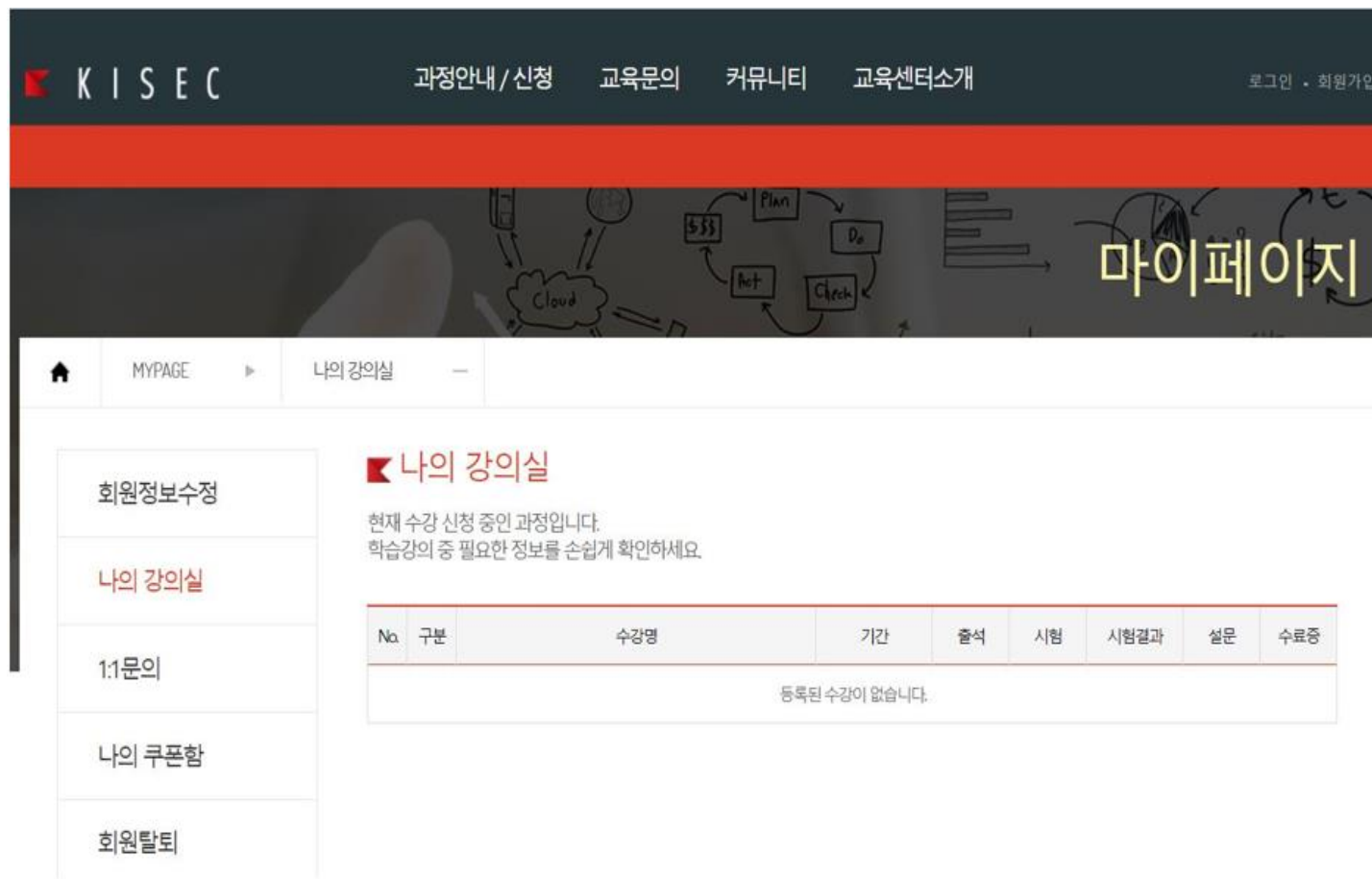
미흡한 인증처리 과정으로 인해 발생하는 취약점으로 공격자가 **인증을 우회하여** 비인가적인 행위를 할 수 있다.

발생 경로

OO

시나리오

Mypage 경로의 URL을 탈취할 경우 공격자는 비로그인 상태에서도 인증을 우회하여 Mypage에 접근할 수 있고 그로 인해 회원정보 유출이 발생한다.

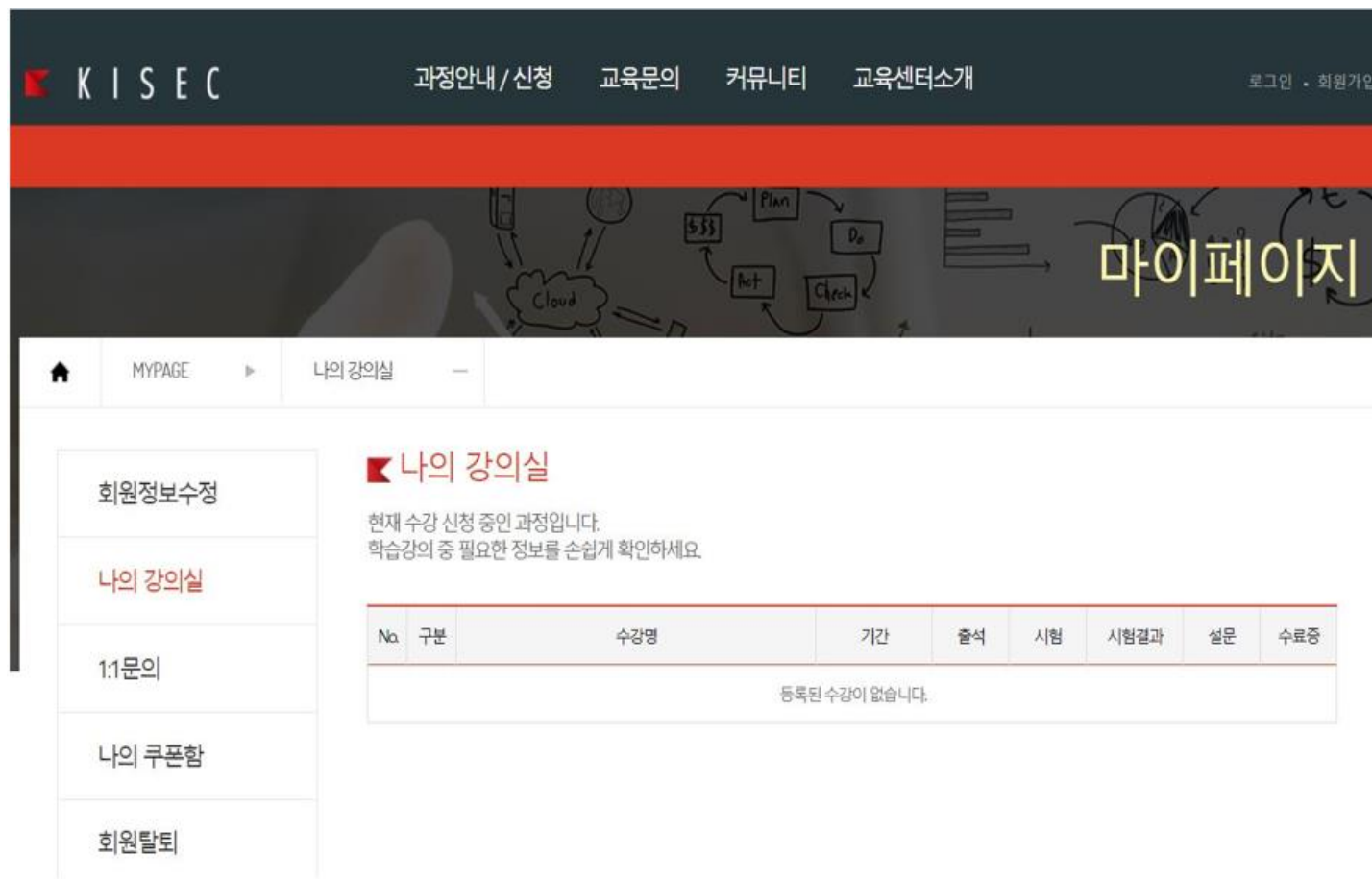


프로세스 검증 누락

미흡한 인증처리 과정으로 인해 발생하는 취약점으로 공격자가 **인증을 우회하여** 비인가적인 행위를 할 수 있다.

보호대책

로그인 권한이 필요한 페이지를 이용할 시 로그인 여부를 확인할 수 있는 세션 값을 설정하여 로그인이 정상적인지 **점검하는 코드를 추가, 인증하여야** 한다.



쿠키 변조

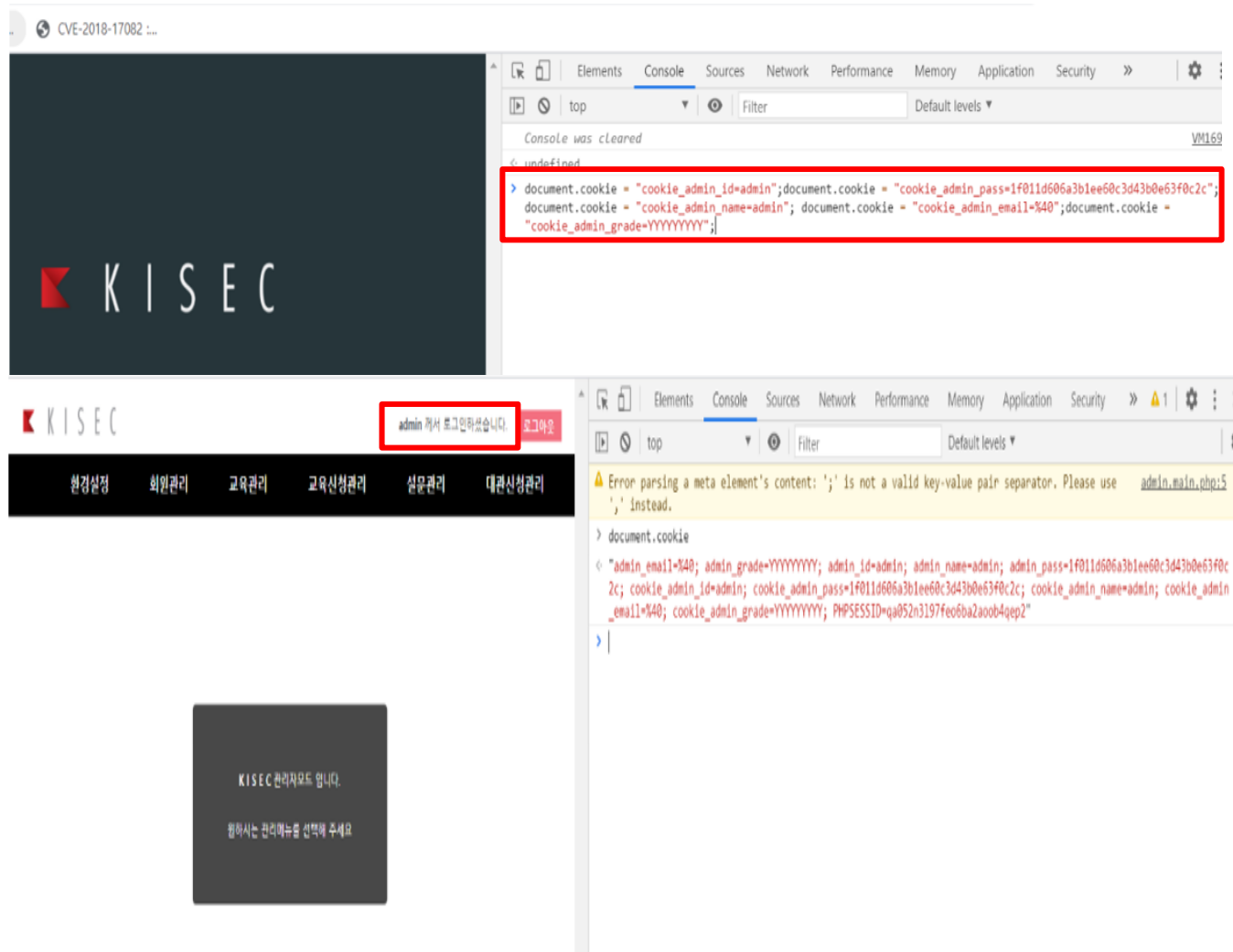
보호되지 않은 쿠키를 사용하여 쿠키 인젝션 등과 같은 **쿠키 값 변조**를 통한 다른 사용자로의 위장 및 권한 상승이 가능하다.

발생 경로

OO

시나리오

공격자가 쿠키 변조를 통해서 관리자 페이지에 접속 권한을 획득 하고 그로 인해 많은 양의 회원정보가 유출될 수 있고 관리자 권한을 이용하여 사이트 내 악성 스크립트를 삽입할 수 있다.



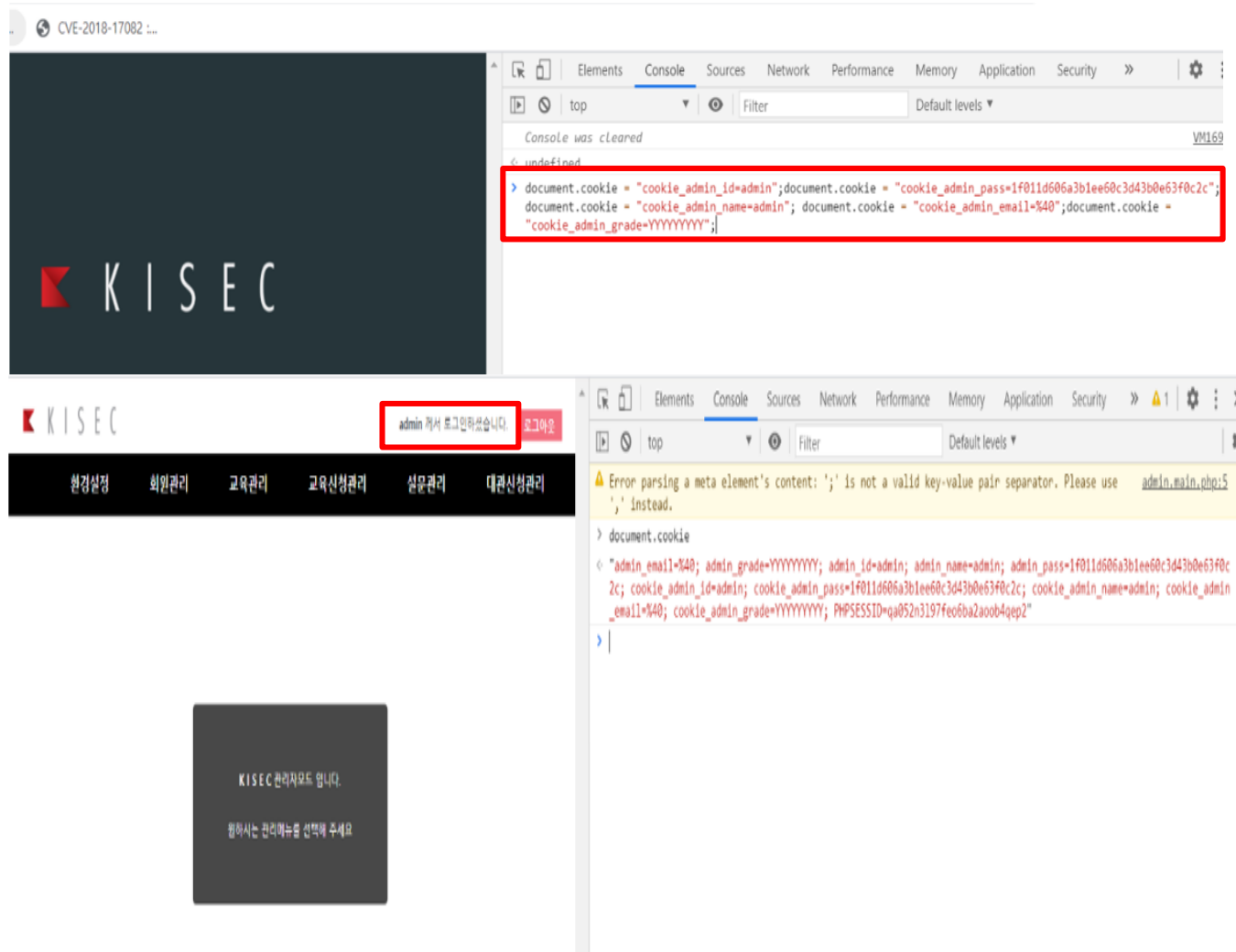
쿠키 변조

보호되지 않은 쿠키를 사용하여 쿠키 인젝션 등과 같은 **쿠키 값 변조**를 통한 다른 사용자로의 위장 및 권한 상승이 가능하다.

보호대책

Cookie를 사용할 경우 SEED, 3DES, AES 등 공인된 암호화 알고리즘을 사용하여 암호화를 적용하고, 가급적이면 Cookie 대신 Session 방식을 사용한다.

클라이언트의 자원을 사용하는 쿠키와는 달리 세션은 서버 쪽의 자원을 사용하고 있어 보안성이 높다고 할 수 있으므로, **세션방식을 채택**하는 것이 바람직하다.



회원정보 유출 및 취약점

01 위험도기준 우선순위

- 크로스 사이트 스크립팅(XSS)
- 데이터 평문 전송
- 쿠키 변조
- 불충분한 인증
- 불충분한 인가
- 세션 고정
- 프로세스 검증 누락

02 가격대비효율 순위

- 크로스 사이트 스크립팅(XSS)
- 불충분한 인가
- 불충분한 인증
- 세션 고정
- 프로세스 검증 누락
- 쿠키 변조
- 데이터 평문 전송

×

홈페이지 취약점

02

디렉토리 인덱싱

웹 디렉토리의 파일 리스트가 웹 브라우저를 통해서 출력되도록 설정되어있는 경우, 중요한 파일을 다운로드하거나 웹사이트 구조를 파악하여 공격에 이용할 수 있는 취약점이다.

발생 경로

OO

시나리오

공격자가 웹상에서 보이지 않는 경로들을 파악하고 악용할 수 있으며 파일 다운로드 취약점을 함께 이용하면 접근이 불가능한 각종 설정 파일들과 웹사이트에 중요한 파일들을 다운로드 하여 민감정보와 소스코드 등을 탈취할 수 있다.

Index of /_core

- [Parent Directory](#)
- [Classes/](#)
- [_common/](#)
- [_community_init.php](#)
- [_csv_download.php](#)
- [_download.php](#)
- [_files/](#)
- [_group_auth.php](#)
- [_init.php](#)
- [_lib/](#)
- [_log/](#)
- [_zipcode/](#)
- [_actionForm.html](#)
- [_coupon_search.php](#)
- [_portfolio_modify.php](#)
- [_type_gugun.php](#)
- [_type_large.php](#)
- [_type_middle.php](#)
- [_type_middle_client.php](#)
- [_type_schedule.php](#)
- [_type_small.php](#)

해당 페이지에서 직접적으로 파일을 다운받을 수 없게 설정되어 있으나 파일 다운로드 취약점과 결합하여 권한이 허락되는 한 서버의 모든 파일을 다운 받을 수 있었다.

디렉토리 인덱싱

웹 디렉토리의 파일 리스트가 웹 브라우저를 통해서 출력되도록 설정되어있는 경우, 중요한 파일을 다운로드하거나 웹사이트 구조를 파악하여 공격에 이용할 수 있는 취약점이다.

보호 대책

- 웹 서버 설정 변경

서버 설정파일에서 아래의 붉은 부분을 제거하여 준다.

파일명: apache.conf or httpd.conf

인덱싱 취약점 존재

```
<Directory />
```

```
Options Indexes FollowSymLinks
```

```
AllowOverride All
```

```
</Directory>
```

Index of /_core

- [Parent Directory](#)
- [Classes/](#)
- [common/](#)
- [community_init.php](#)
- [csv_download.php](#)
- [download.php](#)
- [files/](#)
- [_group_auth.php](#)
- [_init.php](#)
- [_lib/](#)
- [_log/](#)
- [_zipcode/](#)
- [actionForm.html](#)
- [coupon_search.php](#)
- [portfolio_modify.php](#)
- [type_gugun.php](#)
- [type_large.php](#)
- [type_middle.php](#)
- [type_middle_client.php](#)
- [type_schedule.php](#)
- [type_small.php](#)

해당 페이지에서 직접적으로 파일을 다운받을 수 없게 설정되어 있으나 파일 다운로드 취약점과 결합하여 권한이 허락되는 한 서버의 모든 파일을 다운 받을 수 있었다.

파일 다운로드

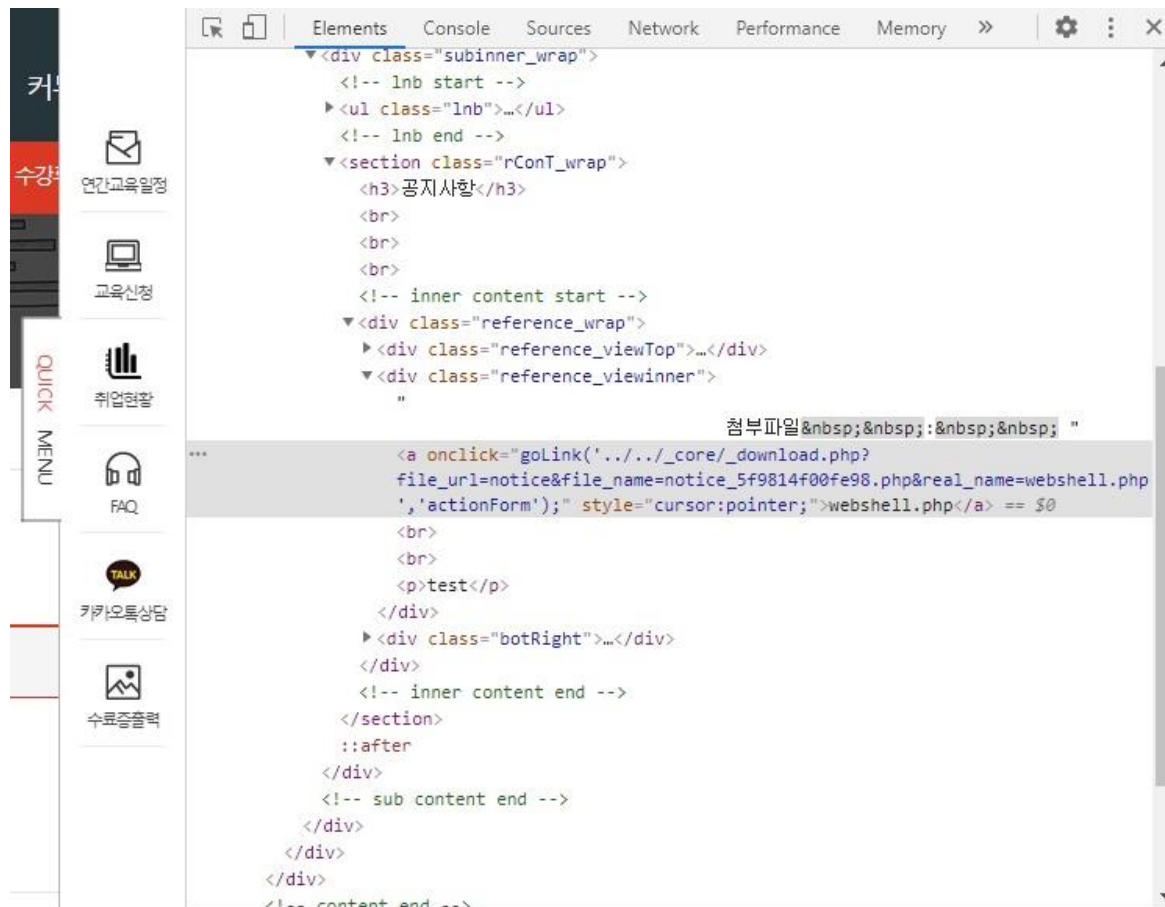
상대경로를 조작해서 다른 파일을 다운받을 수 있다.

발생 경로

OO

시나리오

공격자가 해당 취약점을 이용해 다운로드 권한이 없는 파일을 다운로드하여 해당 파일에 존재하는 민감 정보를 탈취하여 악용할 수 있다. 또한 디렉토리 인덱싱 취약점과 결합시 웹의 소스코드와 민감 정보를 탈취하여 악용할 수 있다.



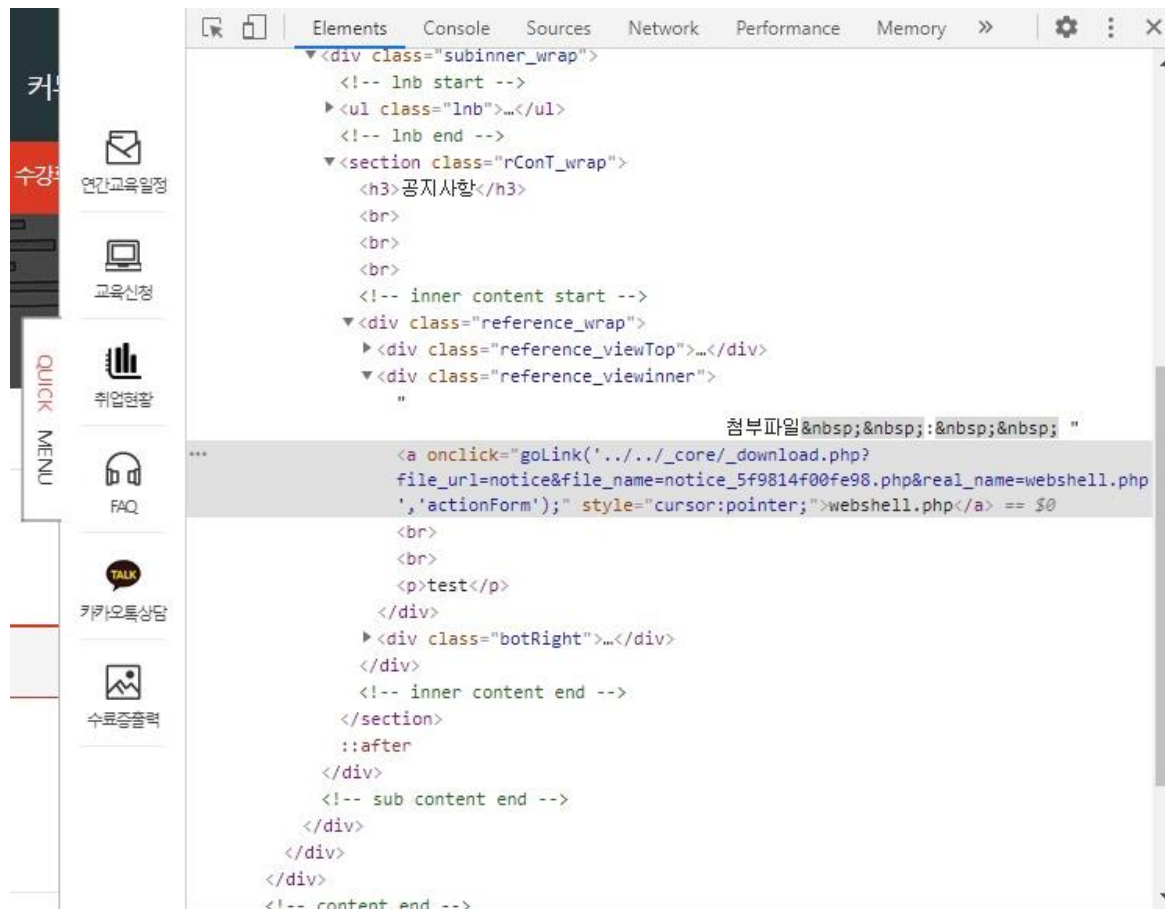
파일 다운로드

상대경로를 조작해서 다른 파일을 다운받을 수 있다.

보호 대책

- 소스코드 수정

다운로드 모듈의 경로를 처리하는 파라미터 변수에 대해서 [../], [..\\], [./]를 필터링해야 한다.



정보누출

웹 사이트의 민감한 정보(소스코드 내 계정 및 비밀번호, 애플리케이션정보, DB정보, 웹서버 구성 정보, 개발 과정의 코멘트 등)가 노출되어 공격자들의 2차 공격을 위한 정보로 활용될 수 있다.

발생 경로

OO

시나리오

노출되는 정보를 기반으로 해커는 해당 버전들의 알려진 취약점들을 파악 할 수 있으며 그로인해 서버의 관리자 권한을 장악 당할 수 있다.

PHP Credits

Exploitdb사이트 DB정보 취약점 검색 후 정보 유출 가능성이 존재 한다.

| PHP Group |
|--|
| Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski, Jim Winstead, Andrei Zmievski |

| Language Design & Concept |
|--|
| Andi Gutmans, Rasmus Lerdorf, Zeev Suraski, Marcus Boerger |

| PHP Authors | |
|--------------------------------|---|
| Contribution | Authors |
| Zend Scripting Language Engine | Andi Gutmans, Zeev Suraski, Stanislav Malyshev, Marcus Boerger, Dmitry Stogov |
| Extension Module API | Andi Gutmans, Zeev Suraski, Andrei Zmievski |
| UNIX Build and Modularization | Stig Bakken, Sascha Schumann, Jani Taskinen |

| | |
|----------------|---|
| Window | 1 HTTP/1.1 200 OK |
| Server / Layer | 2 Date: Mon, 02 Nov 2020 10:49:50 GMT |
| Streams | 3 Server: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.2g PHP/5.3.25 |
| PHP Da | 4 X-Powered-By: PHP/5.3.25 |
| | 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT |
| | 6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 |
| | 7 Pragma: no-cache |
| | 8 Content-Length: 99 |
| | 9 Connection: close |
| | 10 Content-Type: text/html; charset=utf-8 |

정보누출

웹 사이트의 민감한 정보(소스코드 내 계정 및 비밀번호, 애플리케이션정보, DB정보, 웹서버 구성 정보, 개발 과정의 코멘트 등)가 노출되어 공격자들의 2차 공격을 위한 정보로 활용될 수 있다.

보호 대책

- 서버 설정 변경

[php.ini]
expose_php = Off

[apache.conf or httpd.conf]
ServerTokens Prod
ServerSignature Off

PHP Credits

Expoitdb사이트 DB정보 취약점 검색 후 정보 유출 가능성이 존재 한다.

| PHP Group |
|--|
| Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski, Jim Winstead, Andrei Zmievski |

| Language Design & Concept |
|--|
| Andi Gutmans, Rasmus Lerdorf, Zeev Suraski, Marcus Boerger |

| PHP Authors | |
|--------------------------------|---|
| Contribution | Authors |
| Zend Scripting Language Engine | Andi Gutmans, Zeev Suraski, Stanislav Malyshev, Marcus Boerger, Dmitry Stogov |
| Extension Module API | Andi Gutmans, Zeev Suraski, Andrei Zmievski |
| UNIX Build and Modularization | Stig Bakken, Sascha Schumann, Jani Taskinen |

| | |
|----------------|---|
| Window | 1 HTTP/1.1 200 OK |
| Server / Layer | 2 Date: Mon, 02 Nov 2020 10:49:50 GMT |
| Streams | 3 Server: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.2g PHP/5.3.25 |
| PHP Da | 4 X-Powered-By: PHP/5.3.25 |
| | 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT |
| | 6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 |
| | 7 Pragma: no-cache |
| | 8 Content-Length: 99 |
| | 9 Connection: close |
| | 10 Content-Type: text/html; charset=utf-8 |

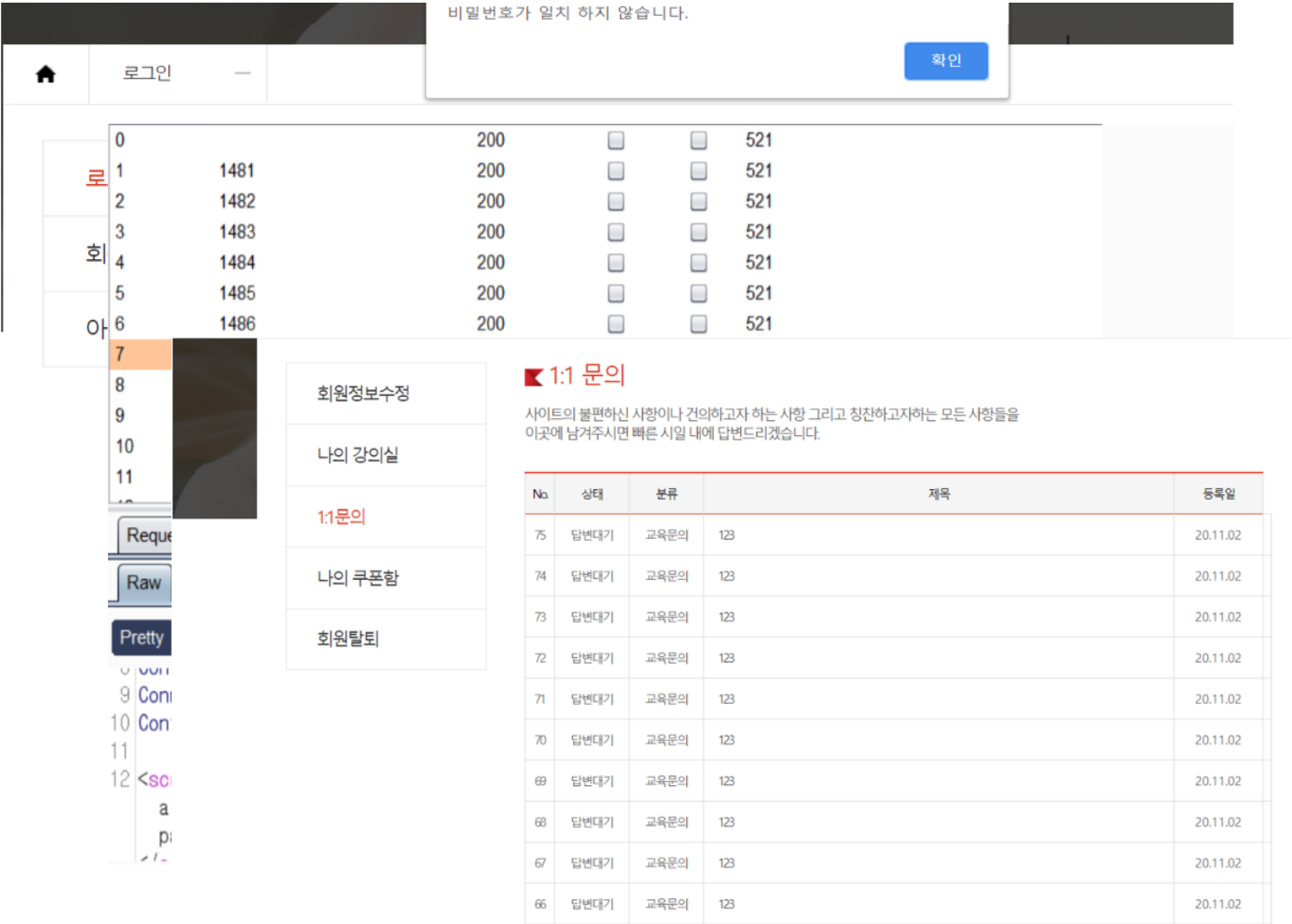
자동화 공격

웹 애플리케이션에 정해진 프로세스에 자동화된 공격을 수행함으로써 자동으로 수많은 프로세스가 진행되는 취약점이다.

발생 경로
OO

시나리오

공격자는무차별 대입을 활용하여 아이디, 패스워드를 크랙할 수 있을 뿐 아니라 악성 게시글을 빠르게 작성하여 서버의 부하를 유발하여 서버 접속을 불안정하게 만들 수 있다.



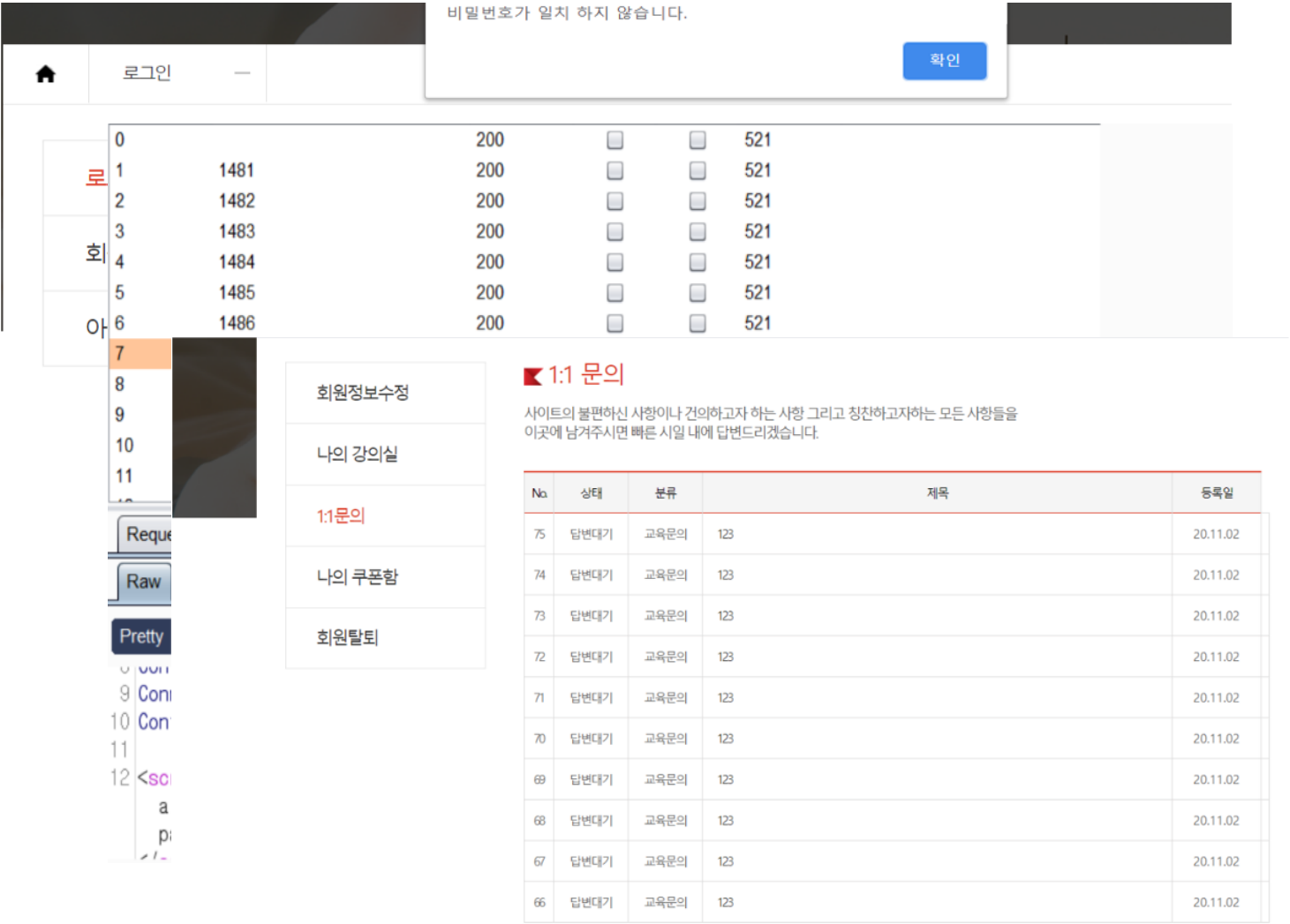
자동화 공격

웹 애플리케이션에 정해진 프로세스에 자동화된 공격을 수행함으로 자동으로 수많은 프로세스가 진행되는 취약점이다.

보호 대책

- 접근시도 횟수 설정

특정 시간 내 동일 프로세스가 반복 실행되지 않도록 **시간제한** 및 **CAPTCHA**인증을 적용하고, 또한, 자동화공격에 의한 시스템 과부하를 방지하기 위한 접근검은 보안 솔루션을 통해 대량의 패킷이 유입되는지 모니터링 해야 한다.



관리자 페이지 노출

홈페이지 관리 기능이 제공되는 관리자 페이지 주소를 추측하여 외부에서 접속할 수 있는 취약점이다.

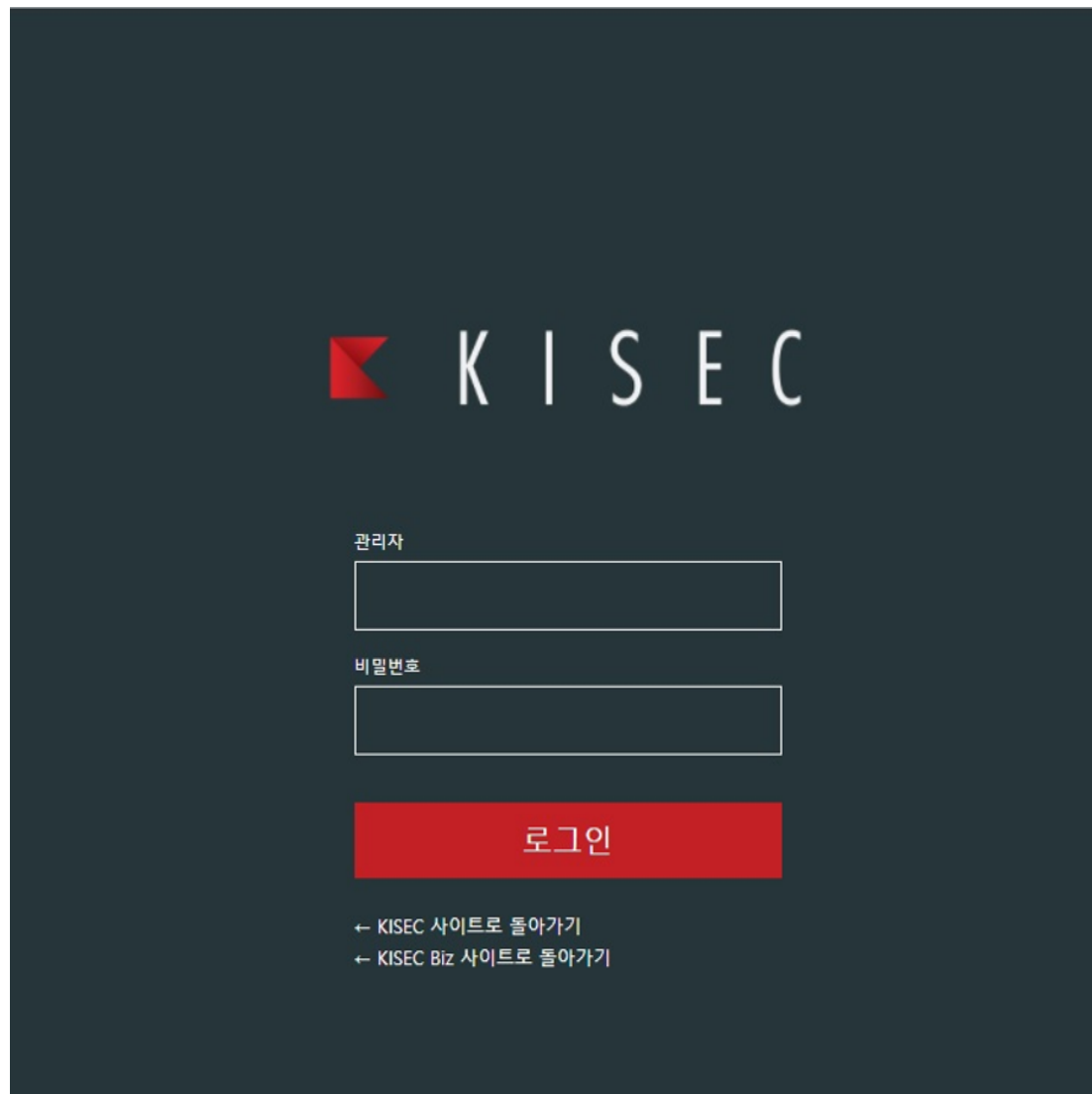
발생 경로

OO

시나리오

공격자가 해당 취약점이 존재하게 되면 손쉽게 외부에서 관리자 페이지에 접속할 수 있게 되고 로그인 성공 시 다량의 회원정보가 저장되어 있기 때문에 악용 가능하다.

또한 쿠키 변조 같은 취약점과 결합하여 접속 권한을 획득하면 다량의 회원정보의 유출이 발생할 수 있다.



관리자 페이지 노출

홈페이지 관리 기능이 제공되는 관리자 페이지 주소를 추측하여 외부에서 접속할 수 있는 취약점이다.

보호 대책

관리자 페이지 분리 및 적절한 접근 통제

1. 관리자 페이지는 일반 사용자용 인터페이스와 **분리**되어 작성되어야 한다. (별도의 포트, 도메인 등)
2. 관리자 페이지는 임의의 위치에서 접근할 수 없도록 적절한 **접근 통제** 절차가 적용되어야 한다. (IP 접근 제어, SMS 인증 등)
3. **추측하기 쉬운** 디렉토리명이나 파일명을 사용해서는 안된다.



불충분한 세션 만료

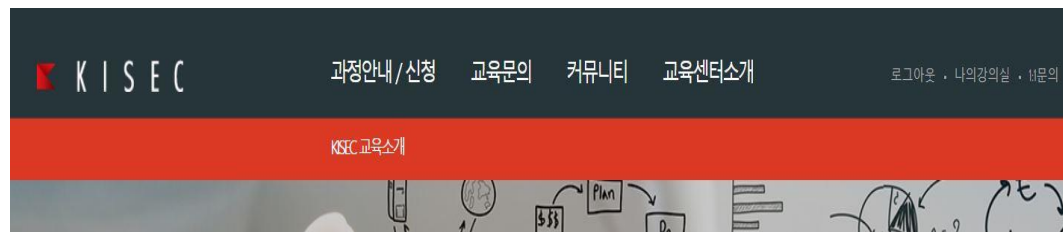
세션의 만료 기간을 정하지 않거나, 만료일자를 너무 길게 설정하여 공격자가 만료되지 않은 세션 활용이 가능하다.

발생 경로

OO

시나리오

공격자가 세션을 탈취하고 악용을 하였을 때 세션이 만료가 되지않아 무기한적으로 해당 계정의 권한을 유지할 수 있어 2차적인 피해가 가능하다.



10분 뒤



불충분한 세션 만료

세션의 만료 기간을 정하지 않거나, 만료일자를 너무 길게 설정하여 공격자가 만료되지 않은 세션 활용이 가능하다.

보호 대책

•세션 타임아웃 설정

세션ID는로그인시 마다 새로운 세션 ID를 발급받도록 하며, 세션 타임아웃 설정을 통해 **일정 시간(10분)** 동안 움직임이 없을 경우 자동 로그아웃 되도록 한다.



10분 뒤



발생 경로

00

시나리오

공격자가 해당 취약점을 이용하여 웹 셸을 첨부파일에 올리고 다른 홈페이지 이용자가 해당 게시물을 클릭한 경우 해당 이용자의 정보들을 탈취하여 악용 가능하다.

게시판 > 게시판관리 > 공지사항 수정

| | | | |
|------------|--|---------|--|
| 표시정보 | 표시 <input type="button" value="표시"/> 공지체크 <input type="checkbox"/> 공지 (체크시 상단에 공 지) | 구분(사이트) | KISEC <input type="button" value="v"/> |
| 작성자 | 전체관리자 | HIT | 0 |
| 제목 | testtest | | |
| 다운로드 파일 #1 | <input type="button" value="파일 선택"/> webserv.php | | |
| 다운로드 파일 #2 | <input type="button" value="파일 선택"/> 선택된 파일 없음 | | |
| 상세내용 | <div style="border: 1px solid gray; padding: 5px;"> <p>글꼴 - 9pt 가 간 가 과 가 - 가 가 URL ※ 사진</p> <hr/> <p>test</p> </div> <div style="margin-top: 10px; text-align: center;"> <input type="button" value="이래 영역을 드래그하여 입력창 크기를 조절할 수 있습니다."/> X </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 5px;"> <> 입력창 크기 조절 Editor HTML TEXT </div> | | |

정보수정

취소

보호 대책

- 소스코드 수정(업로드 확장 확인)

업로드가 허용된 확장자만 가능토록 Server Side에서 컨트롤 해줘야하고 허용할 확장자를 제외한 모든 파일의 업로드를 금지하는 White list 방식의 필터링을 적용해야한다. 또한 확장자 검사를 할 때, 대소문자 구분 없이 비교해야하며 jpg.php 와 같은 이중 확장자나 끝에 "." 을 추가하는 trick에 주의하며 처리해야 한다.

게시판 > 게시판관리 > 공지사항 수정

| | | | |
|------------|--|---------|--|
| 표시정보 | 표시 <input type="button" value="표시"/> 공지체크 <input type="checkbox"/> 공지 (체크시 상단에 공지) | 구분(사이트) | KISEC <input type="button" value="KISEC"/> |
| 작성자 | <input type="text" value="전체관리자"/> | HIT | <input type="text" value="0"/> |
| 제목 | <input type="text" value="testtest"/> | | |
| 다운로드 파일 #1 | <input type="button" value="파일 선택"/> webserv.php | | |
| 다운로드 파일 #2 | <input type="button" value="파일 선택"/> 선택된 파일 없음 | | |
| 상세내용 | <div style="border: 1px solid gray; padding: 5px;"> <p>글꼴 - 9pt 가 간 가 과 가 - < > 가 가 < > < > < > < > URL ※ < > 사진</p> <p>test</p> <p style="text-align: center;">이래 영역을 드래그하여 입력창 크기를 조절할 수 있습니다. ✕</p> </div> <div style="margin-top: 5px; text-align: right;"> <input type="button" value="Editor"/> <input type="button" value="HTML"/> <input type="button" value="TEXT"/> </div> | | |

정보수정

취소

SQL 인젝션

웹 파라미터에 SQL 구문을 이용하여 쿼리를 조작할 수 있는 취약점으로 DB 내의 개인정보가 유출되어 2차공격의 중요한 정보를 제공할 수 있는 취약점이다.

발생 경로

OO

시나리오

SQL 인젝션이 존재하면 공격자가 취약점을 이용하여 데이터베이스의 정보 및 내용을 탈취하여 데이터베이스에 저장되어 있는 사용자들의 아이디, 비밀번호 등 개인정보를 탈취할 수 있다.

The image displays four instances of a web application's search functionality, each demonstrating a successful SQL injection attack. In each case, the search bar contains a malicious query: 'aaaa@kiseccom' and 1=1--', '테스트')>0 union select version()#', '테스트')>0 union select version()#', and '수강')>0 union select version()#'. A red box highlights the error message 'SQL Query 에 문제가 있습니다.' (There is a problem with the SQL Query) displayed below the search bar. A DevTools console error message is also visible in the top right corner of the first instance, stating: 'DevTools failed to load SourceMap: Could not load content 0.166/kiseccom/js/swiper.min.js.map: HTTP error: status code 404, HTTP response code FAILURE'.

SQL 인젝션

웹 파라미터에 SQL 구문을 이용하여 쿼리를 조작할 수 있는 취약점으로 DB 내의 개인정보가 유출되어 2차공격의 중요한 정보를 제공할 수 있는 취약점이다.

보호 대책

- 소스코드 수정(문자 필터)

웹 애플리케이션 개발 시 SQL 인젝션 공격을 유발시킬 수 있는 문자들을 필터링 하여 사용하지 못하도록 한다.
※ addslashes 등 함수 사용

- Database 운영 레벨 수정

DB계정에 최소 권한만을 부여
DB계정에 system 권한(root)을 부여해서는 안된다.

The image displays four screenshots of a web application's search functionality, each demonstrating a successful SQL injection attack. In each case, the search bar contains a query like '테스트')>0 union select version()#' or '수강')>0 union select version()#'. The resulting error message, 'SQL Query 에 문제가 있습니다.', is highlighted with a red box. A DevTools console message at the top right of the first screenshot reads: 'DevTools failed to load SourceMap: Could not load content 0.166/kisec/js/swiper.min.js.map: HTTP error: status code 401, ERR_HTTP_RESPONSE_CODE_FAILURE'.

홈페이지 취약점

01 위험도기준 우선순위

- SQL 인젝션
- 파일 업로드
- 자동화 공격
- 불충분한 세션 만료
- 파일 다운로드
- 관리자 페이지 노출
- 디렉터리 인덱싱
- 정보노출

02 가격대비효율 순위

- SQL 인젝션
- 파일 업로드
- 파일 다운로드
- 불충분한 세션 만료
- 자동화 공격
- 관리자 페이지 노출
- 디렉터리 인덱싱
- 정보노출

모의해킹 2팀

Q&A

THANK
YOU